数理解析研究所講究録 1360 巻 2004 年 5-8

実数値パラメータを含むある計算論における degree について

豊田工業高等専門学校 米澤佳己 (Yoshimi Yonezawa)
yonezawa@math.nagoya-u.ac.jp

§1. 定義と準備

今回の講演における実数値計算論とは Blum, Shub, Smale が [1] において定義した計算論を意味し, 以下で定義される計算機言語によって計算可能な関数全体に関する理論を意味する.

Variable symbols

∘ $N_1, N_2, \ldots$	入出力用整数型変数	∘ $TN_1, TN_2, \ldots$	補助整数型変数
∘ $A_1, A_2, \ldots$	入出力用実数型変数	∘ $TA_1, TA_2, \ldots$	補助実数型変数
∘ $X_1, X_2, \ldots$	入出力用実数値配列型変数	∘ $TX_1, TX_2, \ldots$	補助実数値配列型変数

Statements

(N は整数型変数, A, B, C,B_i $(i = 1, 2, \ldots)$ は実数型変数, Y, Z は実数値配列型変数とする.)

S1) $N := N + 1$	S2) $N := N \dot{-} 1$	S3) IF $N \neq 0$ GOTO j
S4) $A := B + C$	S5) $A := B - C$	S6) $A := B \cdot C$
S7) $A := B/C$	S8) $A := B$	S9) $A := \alpha \quad (\alpha \in \mathbb{R})$
S10) IF $A \leq B$ GOTO j	S11) $A := Y[N]$	S12) $Y[N] := A$
S13) $N := \mathrm{size}(Y)$	S14) $Y := \langle B_1, B_2, \ldots, B_n \rangle$	S15) $Y := \langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle$ $(\alpha_i \in \mathbb{R})$
S16) $\mathrm{size}(Y) := N$	S17) $Y := Z$	S18) END

定義 (B.S.S. recursive function, predicate, set)

- 上の計算機言語で書かれた行番号付きの program により計算可能な関数を B.S.S. recursive function と呼ぶ. また B.S.S. recursive predicate や B.S.S. recursive set とはその range が $\{0, 1\}$ になる total B.S.S. recursive function のことである. (0 を false, 1 を true と解釈する.)
- 集合 S に対して関数 f が B.S.S. recursive in S であるということを, 新しい型の statement

  SO) IF $(x \in \tilde{S})$ GOTO j (但し, $\tilde{S}$ は 集合 S を表す symbol, x は $\tilde{S}$ の型に対応したものとする)

  を導入し, この拡張した計算機言語において計算可能なものとして定義する. (このとき S を oracle, この statement を oracle statement と呼ぶ.)

定義 (Coding, index)

この計算機言語 での program は適当な coding を考えることにより $\langle e, E\rangle$ ($e \in \omega$, $E \in \mathcal{R} = \mathbb{R}^{<\omega}$) という形の code で表される. $\langle e, E\rangle$ をその program が計算している関数の index と呼ぶ.

定義 (Computation path)

関数 f を B.S.S. recursive function in S とし, その index を $\langle e, E\rangle$ であるとする. 関数の入力 $\langle \vec{x}, \vec{\alpha}, \vec{X}\rangle$ に対して, $\langle e, E\rangle$ における計算が T- step で停止するとき, その計算の実行において通過した行番号を列として表したもの $p = \langle n_1, n_2, \ldots, n_T\rangle$ を $\langle e, E\rangle$ における $\langle \vec{x}, \vec{\alpha}, \vec{X}\rangle$ の computation path という.

定義 (B.S.S. r.e. set)

集合 Ω がある B.S.S. recursive function in S の domain になっているとき Ω を B.S.S. r.e. set in S と呼ぶ.

定義 (basic semi algebraic set)

- 関数 $h : \mathfrak{X} \to \mathbb{R}$ $(\mathfrak{X} = \omega^n \times \mathbb{R}^m \times \mathcal{R}^l)$ が分数関数であるとは ω の元を $\mathbb{R}$ の元と解釈し, $\mathcal{R}$ はある $\mathbb{R}^d$ に制限することにより, h が $\mathbb{R}^{n+m+dl}$ 上の分数関数で表されることとする. また $h : \mathfrak{X} \to \mathcal{R}$ が分数関数であるとは $h = \langle h_1, h_2, \ldots\rangle$ の各成分が分数関数であることとする.
- $\mathfrak{X} = \omega^n \times \mathbb{R}^m \times \mathcal{R}^l$ の subset X が basic semi algebraic set であるとは, ある有限個の分数関数 $h_1^1(x), \ldots, h_{n_1}^1(x)$ と $h_1^2(x), \ldots, h_{n_2}^2(x)$ があって

$$x \in X \iff h_1^1(x) > 0 \ \& \ \cdots \ \& \ h_{n_1}^1(x) > 0 \quad \& \quad h_1^2(x) \geq 0 \ \& \ \cdots \ \& \ h_{n_2}^2(x) \geq 0$$

  と表されることとする.

○ S を集合とする. $\mathfrak{X}=\omega^n\times\mathbb{R}^m\times\mathcal{R}^l$ の subset X が basic semi algeraic set in S であるとは, ある有限個の分数関数 $h_1^1(x),\dots,h_{n_1}^1(x)$, $h_1^2(x),\dots,h_{n_2}^2(x)$, $h_1^3(x),\dots,h_{n_3}^3(x)$, $h_1^4(x),\dots,h_{n_4}^4(x)$ があって

$$\begin{aligned} x\in X \iff\ & h_1^1(x)>0\ \&\ \cdots\ \&\ h_{n_1}^1(x)>0 \quad \& \quad h_1^2(x)\geq 0\ \&\ \cdots\ \&\ h_{n_2}^2(x)\geq 0 \\ & \&\ h_1^3(x)\in S\ \&\ \cdots\ \&\ h_{n_3}^3(x)\in S \quad \& \quad h_1^4(x)\notin S\ \&\ \cdots\ \&\ h_{n_4}^4(x)\notin S \end{aligned}$$

と表されることとする.

<u>定理</u> (Normal Form Theorem, Enumeration Theorem, etc.)

○ 述語 $T_{n,m,l}^S(e,E,\vec{x},\vec{\alpha},\vec{X},p)$ を「code $\langle e,E\rangle$ の (oracle S を含む) program に $\langle\vec{x},\vec{\alpha},\vec{X}\rangle$ を入力すると computation path p にしたがって動作し停止する.」を表すものとすると, これは B.S.S. recursive predicate in S である.

○ $C_{n,m,l}^S$: B.S.S. recursive predicate in S と $U_{n',m',l'}$: B.S.S. recursive function が存在し, $f:\mathfrak{X}\to\mathfrak{Y}$ ($\mathfrak{X}=\omega^n\times\mathbb{R}^m\times\mathcal{R}^l$, $\mathfrak{Y}=\omega^{n'}\times\mathbb{R}^{m'}\times\mathcal{R}^{l'}$) が index $\langle e,E\rangle$ の B.S.S. recursive function in S ならば

$$f(\vec{x},\vec{\alpha},\vec{X})=\ U_{n',m',l'}\left(C_{n,m,l}^S(e,E,\vec{x},\vec{\alpha},\vec{X},\mu p[T_{n,m,l}^S(e,E,\vec{x},\vec{\alpha},\vec{X},p)])\right).$$

となる. この右辺を $\{\langle e,E\rangle\}^S(\vec{x},\vec{\alpha},\vec{X})$ と表す.

○ 集合 $\{\mathfrak{A}\mid T_{n,m,l}^S(e,E,\mathfrak{A},p)\}$ を $V_p^{\langle e,E\rangle,S}$ とする. Ω が B.S.S. r.e. set in S であることと, ある $\langle e,E\rangle$ があって

$$\Omega=\bigcup_{p\in\omega}V_p^{\langle e,E\rangle,S}$$

と表されることとは同値.

○ $V_p^{\langle e,E\rangle,S}$ は basic semi algebraic set in S である.

○ $f=\{\langle e,E\rangle\}^S$ であるとき, 各 $p\in\omega$ に対し f の $V_p^{\langle e,E\rangle,S}$ への制限は分数関数として表される.

<u>定理 1</u> $A(\mathfrak{A})$ を $\mathfrak{X}$ 上の predicate とする. 次は同値
(1) $A(\mathfrak{A})$ は B.S.S. r.e. in S である.
(2) ある $\langle e,E\rangle$ があって $A(\mathfrak{A}) \iff \exists p\in\omega\, T_{n,m,l}^S(e,E,\mathfrak{A},p)$
(3) 集合 $A=\{\mathfrak{A}\in\mathfrak{X}\mid A(\mathfrak{A})\}$ はある $\langle e.E\rangle$ があって $A=\bigcup_{p\in\omega}V_p^{\langle e,E\rangle,S}$ と表せる.
(4) ある R: B.S.S. recursive predicate in S があって $A(\mathfrak{A}) \iff \exists n\in\omega\, R(n,\mathfrak{A})$.
(5) ある R: B.S.S. recursive predicate in S があって $A(\mathfrak{A}) \iff \exists\alpha\in\mathbb{R}\, R(\alpha,\mathfrak{A})$.
(6) ある R: B.S.S. recursive predicate in S があって $A(\mathfrak{A}) \iff \exists X\in\mathcal{R}\, R(X,\mathfrak{A})$.

<u>定理</u>
Ω と $\mathfrak{X}-\Omega$ がともに B.S.S. r.e. set であることと Ω が B.S.S. recursive set であることは同値.

§2. B.S.S. Turing Degrees

<u>定義</u>(B.S.S. Turing degree)

○ $A\subseteq\mathfrak{X}$ と $B\subseteq\mathfrak{Y}$ に対し関数 $f:\mathfrak{X}\to\{0,1\}$ で total B.S.S. recursive function in B かつ

$$f(\mathfrak{A})=1 \iff \mathfrak{A}\in A$$

をみたすものが存在するとき, A は B から還元可能であるといい, $A\leq_T^{BSS}B$ と表す.

○ $A\leq_T^{BSS}B$ かつ $B\leq_T^{BSS}A$ を $A\equiv_T^{BSS}B$ と定める.
また $\leq_T^{BSS}B$ かつ $B\not\leq_T^{BSS}A$ を $A<_T^{BSS}B$ と定める.

○ $A\subseteq\mathfrak{X}$ と $B\subseteq\mathfrak{Y}$ に対し $A\not\leq_T^{BSS}B$ かつ $B\not\leq_T^{BSS}A$ であることを A と B は B.S.S. Turing degree の意味で比較不能という.

<u>定理 2</u> A,B を $\mathbb{R}^n$ の subset とする. B が Δ_α^0 set ($\alpha>1$), $A\leq_T^{BSS}B$ ならば A も Δ_α^0 set.

証明:

$A \leq_T^{BSS} B$ なので $f : \mathbb{R}^n \to \{0,1\}$, $f = \{\langle e, E\rangle\}^B$ を total B.S.S. recursive function in B で, $f(x) = 1 \iff x \in A$ をみたすものとする. $\mathbb{R}^n = \bigcup_{p\in\omega} V_p^{\langle e,E\rangle,B}$ である.

各 p に対し, $V_p^{\langle e,E\rangle,B}$ は basic semi algebraic in B なので, ある実係数分数関数からなる不等式系

$$\begin{array}{lcl} h_1^1(x) > 0 \;\&\; \cdots \;\&\; h_{n_1}^1(x) > 0 & \& & h_1^2(x) \geq 0 \;\&\; \cdots \;\&\; h_{n_2}^2(x) \geq 0 \\ \&\; h_1^3(x) \in B \;\&\; \cdots \;\&\; h_{n_3}^3(x) \in B & \& & h_1^4(x) \notin B \;\&\; \cdots \;\&\; h_{n_4}^4(x) \notin B \end{array}$$

によって定義される. よって B が Δ_α^0 であることより $V_p^{\langle e,E\rangle,B}$ も Δ_α^0 set になる. 故に

$$\begin{aligned} x \in A &\iff \exists p[f(x) = 1 \;\&\; x \in V_p^{\langle e,E\rangle,B}] \\ x \notin A &\iff \exists p[f(x) = 0 \;\&\; x \in V_p^{\langle e,E\rangle,B}] \end{aligned}$$

となるが f は $V_p^{\langle e,E\rangle,B}$ 上で分数関数で表されるので,(ある閉集合を除いて連続であるから) A および A^c は Σ_α^0 set になり, それゆえに A は Δ_α^0 である. ∎

<u>定理 3</u> $Q \subseteq \mathbb{R}$ を高々可算な集合, $C \subseteq \mathbb{R}$ を非可算 measure 0 集合 [または meager set] とすると $C \not\leq_T^{BSS} Q$.

証明に必要な補題を二つ述べる.

<u>補題 3.1</u> $h : \mathbb{R} \to \mathbb{R}$ を定数でない分数関数, Q を可算集合とすると, $\{x \in \mathbb{R} \mid h(x) \in Q\}$ は高々加算な集合である.

<u>補題 3.2</u> $f : \mathbb{R} \to \mathbb{R}$, $f = \{\langle e, E\rangle\}^B$ を total function でその range が有限集合であるものとする. このとき $V_p^{\langle e,E\rangle,B}$ が無限集合ならば, f は $V_p^{\langle e,E\rangle,B}$ 上定数関数である.

<u>定理 3 の証明:</u>

$C \leq_T^{BSS} Q$ と仮定する. $f : \mathbb{R} \to \{0,1\}$, $f = \{\langle e, E\rangle\}^Q$, total function を, $f(x) = 1 \iff x \in C$ をみたすものとする. $\mathbb{R} = \bigcup_{p\in\omega} V_p^{\langle e,E\rangle,Q}$ であるから, ある $p \in \omega$ に対し $V_p^{\langle e,E\rangle,Q} \cap C$ は非可算集合になる. $V_p^{\langle e,E\rangle,Q}$ の定義不等式系

$$\begin{array}{lcl} h_1^1(x) > 0 \;\&\; \cdots \;\&\; h_{n_1}^1(x) > 0 & \& & h_1^2(x) \geq 0 \;\&\; \cdots \;\&\; h_{n_2}^2(x) \geq 0 \\ \&\; h_1^3(x) \in Q \;\&\; \cdots \;\&\; h_{n_3}^3(x) \in Q & \& & h_1^4(x) \notin Q \;\&\; \cdots \;\&\; h_{n_4}^4(x) \notin Q \end{array}$$

において, 各分数関数は定数関数でないと仮定してよい. すると $h_i^3(x) \in Q$ なる x の集合は高々可算な集合になるので $h_i^3(x) \in Q$ の形をした式は含まない. さらに, 上の不等式系のうち $h_j^2(x) \geq 0$ の形をした式の等号を除いた

$$\begin{array}{lcl} h_1^1(x) > 0 \;\&\; \cdots \;\&\; h_{n_1}^1(x) > 0 & \& & h_1^2(x) > 0 \;\&\; \cdots \;\&\; h_{n_2}^2(x) > 0 \\ & \& & h_1^4(x) \notin Q \;\&\; \cdots \;\&\; h_{n_4}^4(x) \notin Q \end{array}$$

によって定まる集合を V' とすれば $V' \subseteq V_p^{\langle e,E\rangle,Q}$ かつその差は高々有限集合となるので V' もまた非可算集合. V' は空でない開集合から高々加算な点を除いた形になっているので C が measure 0 [または meager set] であることより $V' - C \neq \emptyset$ となる. よって $V_p^{\langle e,E\rangle,Q} \cap C \neq \emptyset$, $V_p^{\langle e,E\rangle,Q} - C \neq \emptyset$ となって $f(x)$ が $V_p^{\langle e,E\rangle,Q}$ 上定数関数であることに反する. ∎

<u>系</u> C を Cantor set, $\mathbb{Q}$ を有理数全体の集合とすると C と $\mathbb{Q}$ は B.S.S. Turing degree の意味で比較不能.

<u>定義</u> $\overline{\mathbb{Q}}$ = 実代数的数の全体 とし, $\mathcal{K} = \{\mathbb{Q}(\alpha) \mid \alpha \in \overline{\mathbb{Q}}\}$ (すなわち, $\mathbb{Q}$ の実有限次拡大体全体) とする.

<u>定理 4</u> $\mathcal{K}$ の元 K と L に対し, $K \subseteq L \iff K \leq_T^{BSS} L$.

証明は二つの部分 Part1: $K \subseteq L \Rightarrow K \leq_T^{BSS} L$ と Part2: $K \leq_T^{BSS} L \Rightarrow K \subseteq L$ の部分に分けて示す.

<u>Part1 の証明:</u>

$K \subseteq L$, $K = \mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_m]$, $L = \mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_n]$, ($\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_n$ は $\mathbb{Q}$ 上一次独立) として K を受理する (L を oracle として持った) program を構成する.

IF $x \notin L$ **THEN output** 0 **END**
$x \in L$ より $x = s + t_1\alpha_1 + \cdots + t_m\alpha_m + u_1\beta_1 + \cdots + u_n\beta_n$ なる有理数 $s, t_1, \ldots, t_m, u_1, \ldots, u_n$ を探す.
IF $u_1 = u_1 = \cdots = u_n = 0$ **THEN output** 1 **ELSE output** 0
END

<u>補題 4.1</u>　$L \in \mathcal{K}$, $h(x)$ を実係数分数関数で、無限に多くの有理数 r に対して $h(r) \in L$ となるものとする. このとき $h(x)$ は L 係数の分数関数である.

<u>証明:</u>

$h(x) = f(x)/g(x)$, ($f(x)$, $g(x)$ は多項式) とし $n = \deg(f) + \deg(g)$ に関する数学的帰納法によって示す.
$n = 0$ の時は明らか.
$n > 0$ の時, 逆数を考えることにより $\deg(f) \geq \deg(g)$ と仮定してよい. $h(r) = q$ とすると

$$h(x) = (f(x) - qg(x))/g(x) + q = (x - r)f_1(x)/g(x) + q$$

となるので $f_1(x)/g(x)$ に帰納法の仮定を用いればよい.

<u>補題 4.2</u>　$L \in \mathcal{K}$, $h(x)$ を実係数分数関数とする. ある $\alpha \notin L$ と相異なる二つの有理数 q_1, q_2 に対し,

$$\exists^\infty r \in \mathbb{Q}[h(r + q_i\alpha) \in L] \qquad (i = 1, 2)$$

をみたすならば, $h(x)$ は定数関数である.

<u>証明:</u>

分数関数 $h(x + q_i\alpha)$ が無限個の有理数 r について L に値を取るので前補題よりこれは L 係数の分数関数. よって $h(x) = p_i(x - q_i\alpha)$, ($p_i(x)$ は L 係数分数関数, $i = 1, 2$) と表される. $p_1(x + q_1\alpha) = p_2(x + q_2\alpha)$ なので x に $x - q_1\alpha$ を代入すると $p_1(x) = p_2(x + q\alpha)$ ($q = q_2 - q_1 \neq 0$) となる. この両辺の係数を比較することにより $p_1(x)$ つまりは $h(x)$ が定数であることがわかる.

<u>Part2 の証明:</u>

$K \leq_T^{BSS} L$ かつ $K \not\subseteq L$ として矛盾を導く. $f : \mathbb{R} \to \{0, 1\}$ を $f = \{\langle \epsilon, E\rangle\}^L$, total,
$f(x) = 1 \iff x \in K$
をみたすものとする. $\mathbb{R} = \bigcup_{p \in \omega} V_p^{\langle \epsilon, E\rangle, L}$ であるから, ある $p \in \omega$ に対し $V_p^{\langle \epsilon, E\rangle, L}$ は非可算集合になる. 明らかに $V_p^{\langle \epsilon, E\rangle, L} - K \neq \emptyset$ である. $V_p^{\langle \epsilon, E\rangle, L}$ の定義不等式系

$$h_1^1(x) > 0 \ \& \ \cdots \ \& \ h_{n_1}^1(x) > 0 \qquad \& \qquad h_1^2(x) \geq 0 \ \& \ \cdots \ \& \ h_{n_2}^2(x) \geq 0$$
$$\& \ h_1^3(x) \in L \ \& \ \cdots \ \& \ h_{n_3}^3(x) \in L \qquad \& \qquad h_1^4(x) \notin L \ \& \ \cdots \ \& \ h_{n_4}^4(x) \notin L$$

において, 各分数関数は定数関数でないと仮定してよい. すると $h_i^3(x) \in L$ なる x の集合は高々可算な集合になるので $h_i^3(x) \in L$ の形をした式は含まない. U を

$$h_1^1(x) > 0 \ \& \ \cdots \ \& \ h_{n_1}^1(x) > 0 \qquad \& \qquad h_1^2(x) > 0 \ \& \ \cdots \ \& \ h_{n_2}^2(x) > 0$$

で定まる集合とし, W を $h_1^4(x) \notin L \ \& \ \cdots \ \& \ h_{n_4}^4(x) \notin L$ で定まる集合すると, $V_p^{\langle \epsilon, E\rangle, L}$ が非可算集合であることより $U \cap W$ は空でない.

<u>Claim</u> $U \cap W \cap K \neq \emptyset$

もし $U \cap W \cap K$ が空だとすると, $x \in U \cap K \Rightarrow h_1^4(x) \in L \ \vee \ \cdots \ \vee \ h_{n_4}^4(x) \in L$ となる. そこで, $\alpha \in U \cap (K - L)$ を一つ取り $x = r + q\alpha \in U \cap K$ ($r, q \in \mathbb{Q}$) を考えると, ある j と q_1, $q_2 (q_1 \neq q_2)$ があって $i = 1, 2$ に対し $h_j^4(r + q_i\alpha) \in L$ なる $r \in \mathbb{Q}$ が無限に存在することがわかるので補題 4.2 より $h_j(x)$ は定数関数となり仮定に反する.

$U \cap W \cap K \neq \emptyset$ と $U \cap W \subseteq V_p^{\langle \epsilon, E\rangle, L}$ から $V_p^{\langle \epsilon, E\rangle, L} \cap K \neq \emptyset$ となり, $V_p^{\langle \epsilon, E\rangle, L} - K \neq \emptyset$ とあわせて $f(x)$ が $V_p^{\langle \epsilon, E\rangle, L}$ 上定数関数であること (補題 3.2) に反する. ∎

<u>References</u>

[1] Blum, L., M. Shub, and S. Smale, "On a Theory of Computation and Complexty over the Real Numbers: NP–Completeness, Recursive Functions and Universal Machines,", Bull. AMS**21**(1989). 1–46.

[2] Blum, L., and S. Smale, "The Gödel Incompletenesss Theorem and Decidability over a Ring," From Topology to Computation:, Proceeding of the Smalefest.

[3] Blum, L., F. Cucker, M. Shub, and S. Smale, Complexity and Real Computation, Splinger, 1998.

[4] Y. Yonezawa, The Normal Form Theorem for the Blum–Shub–Smale's real valued computation theory, 豊田高専紀要 Vol 30